UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

UNITED STATES OF AMERICA, Plaintiff, v. Ryan Jaris Gibson, Defendant.	Court File No. 14-cr-301 (RHK/LIB) (1) **REPORT AND RECOMMENDATION**

This matter came before the undersigned United States Magistrate Judge upon Defendant Ryan Jaris Gibson's ("Defendant") Motion to Suppress Any Evidence Obtained as a Result of Any Illegal Searches, [Docket No. 16], and Motion to Suppress Statements, [Docket No. 17]. This case has been referred to the undersigned Magistrate Judge for a report and recommendation, in accordance with 28 U.S.C. § 636(b)(1) and Local Rule 72.1. The Court held a motions hearing on October 27, 2014, regarding Defendant's pretrial motions.

For reasons discussed herein, the Court recommends that Defendant's Motion to Suppress Any Evidence Obtained as a Result of Any Illegal Searches, [Docket No. 16], and Motion to Suppress Statements, [Docket No. 17], be **DENIED**.

I. BACKGROUND

A. Background

Defendant is charged with one count of possession of child pornography, in violation 18 U.S.C. §§ 2252(a)(4)(B), 2252(b)(2), and 2253. (Indictment [Docket No. 1]).

II. DEFENDANT'S MOTION TO SUPPRESS ANY EVIDENCE OBTAINED AS A RESULT OF ANY ILLEGAL SEARCHES, [DOCKET NO. 16]

Defendant first moves the Court to suppress physical evidence obtained as a result of any search or seizure in the present case, arguing that both search warrants, (Gov't.'s Exs. 2 and 3), were issued without sufficient showings of probable cause. (See Def.' Motion to Suppress Any Evidence Obtained as a Result of Any Illegal Searches, [Docket No. 16]).

As initially submitted, Defendant's motion specifically asserted that the affidavits submitted in support of the applications for the search warrants for his residence, his person, and his place of employment did not provide probable cause because the only information contained in the affidavits linking images of child pornography to his home computer consisted of an specific Internet Protocol ("IP") address, and because the drafter of the affidavits omitted material information, namely, whether Defendant's internet service provider uses static or dynamic IP addresses for its subscribers. (See Id. at 2).

At the motions hearing, Defendant orally withdrew the portion of his motion that argued material omissions had been made in the drafting of the affidavits supporting the applications for the search warrants. Defense counsel also stated on the record that the present motion is limited to a "four-corners" review concerning the sufficiency of the probable cause articulated in each of the search warrant applications' supporting affidavits.[1]

A. Standard of Review

The Fourth Amendment guarantees the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," and that "no warrants shall issue, but upon probable cause, supported by Oath or affirmation." U.S. Const. Amend. IV. The Eighth Circuit has held that "[a]n affidavit establishes probable cause for a warrant if it sets

[1] The parties declined the opportunity to submit additional briefing regarding the motion.

forth sufficient facts to establish that there is a fair probability that contraband or evidence of criminal activity will be found in the particular place to be searched." United States v. Mutschelknaus, 592 F.3d 826, 828 (8th Cir. 2010) (internal quotation marks and citation omitted). "Probable cause is a fluid concept that focuses on 'the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act.'" United States v. Colbert, 605 F.3d 573, 576 (8th Cir. 2010) (quoting Illinois v. Gates, 462 U.S. 213, 231 (1983)). Courts use a "totality of the circumstances test . . . to determine whether probable cause exists." United States v. Hager, 710 F.3d 830, 836 (8th Cir. 2013) (citation omitted).

As alluded to above, the sufficiency of a search warrant affidavit is examined using "common sense and not a hypertechnical approach." United States v. Grant, 490 F.3d 627, 632 (8th Cir. 2007) (citation and internal quotations omitted). "In ruling on a motion to suppress, probable cause is determined based on 'the information before the issuing judicial officer.'" United States v. Smith, 581 F.3d 692, 694 (8th Cir. 2009) (quoting United States v. Reivich, 793 F.2d 957, 959 (8th Cir. 1986)). "Therefore, '[w]hen the [issuing judge] relied solely upon the supporting affidavit to issue the warrant, only that information which is found in the four corners of the affidavit may be considered in determining the existence of probable cause.'" United States v. Wiley, No. 09-cr-239 (JRT/FLN), 2009 WL 5033956, at *2 (D. Minn. Dec. 15, 2009) (Tunheim, J.) (quoting United States v. Solomon, 432 F.3d 824, 827 (8th Cir. 2005); edits in Wiley). In addition, "[a] magistrate's 'determination of probable cause should be paid great deference by reviewing courts,'" Gates, 462 U.S. at 236 (quoting Spinelli v. United States, 393 U.S. 410, 419 (1969)). "[T]he duty of a reviewing court is simply to ensure that the magistrate

had a 'substantial basis for . . . [concluding]' that probable cause existed." Id. at 238-39 (quoting Jones v. United States, 362 U.S. 257, 271 (1960)).

B. The Warrants Background

There are two challenged search warrant applications in the present case, both of which were drafted by Duluth Police Department Investigator Jeanine Pauly[2] on May 22, 2014. (Gov't. Ex. 1, 10; Gov't. Ex. 2, 10). The probable cause statements in the affidavits supporting the applications for the warrants are identical. (See Gov't. Ex. 1, 7-10; Gov't. Ex. 2, 7-10). Based on the information provided in Investigator Pauly's affidavits in support of the applications for the search warrants, the Court concludes that the issuing judge had a substantial basis upon which to conclude that probable cause existed to issue both the May 22, 2014, search warrants for Defendant's residence, his place of employment, and his person.

In her affidavits in support of the two search warrant applications, Investigator Pauly states that, between March 1 and April 7, 2014, Minnesota Child Exploitation Task Force Officer Dale Hansen used an undercover investigative software (UIS) program to download peer to peer files from computers that were later determined to be at Defendant's residence and Defendant's workplace. (Gov't. Ex. 2 at 7-9; Gov't. Ex. 3 at 7-9).

The UIS program is a specially modified peer-to-peer ("P2P") file sharing program. (Gov't. Ex. 2 at 7; Gov't. Ex. 3 at 7). Law enforcement officers use the UIS program nationwide in investigations concerning P2P file sharing. (Gov't. Ex. 2 at 7; Gov't. Ex. 3 at 7). The UIS program has been modified for the needs of law enforcement investigations. (Gov't. Ex. 2 at 7; Gov't. Ex. 3 at 7). The UIS program is designed to connect to computers running P2P programs on file sharing networks. (Gov't. Ex. 2 at 7; Gov't. Ex. 3 at 7). Using the UIS program, an

[2] Investigator Jeanine Pauly is a sworn law enforcement officer currently employed by the Duluth Police Department, and assigned to the Lake Superior Forensic Technology & Internet Crimes Against Children Task Force.

officer connects to a computer on a file sharing network that is hosting files that have been predetermined by the Internet Crimes Against Children Federal Task Force to be child pornography. (Gov't. Ex. 2 at 7; Gov't. Ex. 3 at 7). The affidavit refers to such files as "payloads" of files. (See Gov't. Ex. 2 at 7; Gov't. Ex. 3 at 7). The modifications to the UIS program cause it to download target files from only a single host computer and to document the source of each downloaded file. (Gov't. Ex. 2 at 7; Gov't. Ex. 3 at 7). The UIS program follows the programming language protocols set forth in the public P2P protocol standards and uses only publically available options. (Gov't. Ex. 2 at 7; Gov't. Ex. 3 at 7). No functionality outside the publically available protocols has been added to the UIS program, which eliminates the possibility that investigating officers using the UIS program will intrude on the targeted IP address's private computer files. (Gov't. Ex. 2 at 7; Gov't. Ex. 3 at 7).

Officer Hansen used the UIS program to query computers on a P2P network and request peers that possessed certain files that had previously been identified as child pornography. (Gov't. Ex. 2 at 7; Gov't. Ex. 3 at 7). The P2P servers identified a computer at IP address 71.83.33.81 as possessing some of the requested files. (Gov't. Ex. 2 at 7; Gov't. Ex. 3 at 7). Between March 1 and April 7, 2014, Officer Hansen used the UIS program to attempt to download the suspect files from the host computer at IP address 71.83.33.81. (Gov't. Ex. 2 at 7; Gov't. Ex. 3 at 7). The UIS program was able to partially download two payloads of such files from that computer. (See Gov't. Ex. 2 at 7-8; Gov't. Ex. 3 at 7-8).

The first payload is described as a twelve minute fourteen second long video file depicting a prepubescent female in a dress dancing in front of a professional backdrop and the top of her dress comes down during the video exposing the female's bare chest to the camera. (Gov't. Ex. 2 at 8; Gov't. Ex. 3 at 8). The host computer at IP address 71.83.33.81 possessed all

of the pieces of the complete file. (Gov't. Ex. 2 at 8; Gov't. Ex. 3 at 8). However, the UIS program downloaded copies of only a portion of the pieces necessary to recreate the entire file. (Gov't. Ex. 2 at 8; Gov't. Ex. 3 at 8).

The second payload was described as three video files and a subfolder named "Extras" that contained jpeg[3] images of prepubescent females in lingerie, posing for the camera. (Gov't. Ex. 2 at 8; Gov't. Ex. 3 at 8). The host computer at IP address 71.83.33.81 possessed only a portion of the pieces of the entire "payload" of files. (Gov't. Ex. 2 at 8; Gov't. Ex. 3 at 8). The UIS program downloaded copies of all of the pieces on the host computer. (Gov't. Ex. 2 at 8; Gov't. Ex. 3 at 8). The pieces downloaded by the UIS were sufficient to completely download six files. (Gov't. Ex. 2 at 8; Gov't. Ex. 3 at 8).

Using administrative subpoenas, the officers discovered that, between November 2, 2013, and April 20, 2014, IP address 71.83.33.81 had been assigned to an account in Defendant's name which listed his address at 331 North 28th Avenue West, Apartment 2 ("Defendant's residence"), in Duluth, Minnesota. (Gov't. Ex. 2 at 8; Gov't. Ex. 3 at 8).

Investigator Pauley queried the Minnesota Predatory Offender registration database for Defendant's name. (Gov't. Ex. 2 at 8; Gov't. Ex. 3 at 8). She discovered that Defendant had been convicted in 2006 in Florida of criminal sexual conduct involving a sixteen year old girl. (Gov't. Ex. 2 at 8; Gov't. Ex. 3 at 8). Pursuant to that conviction, Defendant is required to maintain registration as a Predatory Offender for the rest of his life. (Gov't. Ex. 2 at 8; Gov't. Ex. 3 at 8).

While reviewing Defendant's offender status, Investigator Pauley noted that Defendant has been employed since February 1, 2013, at Computer Renaissance, a business located at 2208 Mountain Shadow Drive in Duluth, Minnesota. (Gov't. Ex. 2 at 8; Gov't. Ex. 3 at 8).

[3] A jpeg file is a computer file for the "storage and display of digitized photographic images and photo-realistic art work." United States v. Terry, 240 F. Supp. 2d 922, 930 (S.D. Iowa 2002).

Officer Hansen had also conducted previous P2P network investigations where he received copies of payload files from a computer associated with IP address 24.158.30.34. (Gov't.Ex. 2 at 8; Gov't.Ex. 3 at 8). As part of both that previous investigation and the most recent investigation, Officer Hansen downloaded copies of payload files from this second computer on April 15 and April 17, 2013, and April 4, 2014. (Gov't. Ex. 2 at 8; Gov't. Ex. 3 at 8).

Using administrative subpoenas in 2013 and 2014, the officers discovered that the IP address 24.158.30.34 was assigned to Computer Renaissance with a listed address of 2208 Mountain Shadow Drive, Duluth, Minnesota on April 15 and April 17, 2013, and April 4, 2014 (Gov't. Ex. 2 at 9; Gov't. Ex. 3 at 9). Officer Hansen downloaded two sets of payload files from the host computer at IP address 24.158.30.34. (Gov't. Ex. 2 at 9; Gov't. Ex. 3 at 9).

The first payload set is described as a folder containing 250 images that depict a partially-clothed to nude female who is between twelve and fourteen years old, posing for the camera. (Gov't. Ex. 2 at 9; Gov't. Ex. 3 at 9). In at least one image, the female's genitalia and anus are exposed to the camera. (Gov't. Ex. 2 at 9; Gov't. Ex. 3 at 9). The host computer at IP address 24.158.30.34 possessed all of the pieces of the payload files. (Gov't. Ex. 2 at 9; Gov't. Ex. 3 at 9). Using the UIS program, Officer Hansen downloaded only a portion of the total pieces making up the payload files. (Gov't. Ex. 2 at 9; Gov't. Ex. 3 at 9). The downloaded copies, however, represented fifteen complete files of the payload set from the host computer. (See Gov't. Ex. 2 at 9; Gov't. Ex. 3 at 9).

The second payload set is described as four jpeg images. (Gov't. Ex. 2 at 9; Gov't. Ex. 3 at 9). Two of the images depict a female between the ages of thirteen and fifteen in a bikini, posing for the camera. (Gov't. Ex. 2 at 9; Gov't. Ex. 3 at 9). The host computer at 24.158.30.34

possessed most of the pieces making up the payload set. (Gov't. Ex. 2 at 9; Gov't. Ex. 3 at 9). Using the UIS program, Officer Hansen downloaded only a portion of the pieces on the host computer. (Gov't. Ex. 2 at 9; Gov't. Ex. 3 at 9). The downloaded copies represented two complete files of the four images making up the payload. (Gov't. Ex. 2 at 9; Gov't. Ex. 3 at 9).

On May 6, 2104, Officer Hansen informed Investigator Pauley of the results of his investigation, his belief that the host computers located at IP address 71.83.33.81 and IP address 21.158.30.34 were related, and his belief that both computers were being used by Defendant. (Gov't. Ex. 2 at 9; Gov't. Ex. 3 at 9). Investigator Pauly checked the Duluth Police Department Records and confirmed the Defendant's address as 331 North 28th Avenue West, Apartment 2, in Duluth, his employment at Computer Renaissance at 2208 Mountain Shadow Drive in Duluth, and his status as a registered predatory offender. (Gov't. Ex. 2 at 9; Gov't. Ex. 3 at 9). Investigator Pauly also spoke with Defendant's probation officer. (Gov't. Ex. 2 at 10; Gov't. Ex. 3 at 10). The probation officer informed Investigator Pauly that Defendant was at that time on probation due to his conviction of sexual assault of a minor in Florida, lived at the address on file with the police department, and was prohibited both from possessing pornography and having internet access at his home as conditions of his probation. (Gov't. Ex. 2 at 10; Gov't. Ex. 3 at 10).

On May 12, 2014, Investigator Pauly reviewed and confirmed the data Officer Hansen had downloaded from the host computers at IP address 71.83.33.81 and IP address 24.158.30.34. (Gov't. Ex. 2 at 10; Gov't. Ex. 3 at 10). On May 22, 2014, Minnesota State District Court Judge Gary Larson issued search warrants for Defendant's residence, Defendant's place of employment, and Defendant's person. (Gov't. Ex. 2 at 10; Gov't. Ex. 3 at 10).

C. Analysis

Defendant first argues that the references in the affidavits to the IP addresses are not sufficient to create a nexus between the computers hosting images of child pornography and his home. In the portion of Investigator Pauly's search warrant applications that detail her training and experience, however, she expressly states that she was aware that an IP address can be traced to a physical location where the device for communicating over the internet can be found. (See Gov't. Ex. 2, 4; Gov't. Ex. 3, 4). It is the law of this circuit that, for the purposes of determining whether probable cause exists to search a computer, an IP address assigned to a specific user at the time illegal internet activity associated with that IP address occurs is a sufficient basis to find a nexus between the unlawful use of the internet at that IP address and a computer possessed by the subscriber assigned the address. See, e.g., United States v. Stults, 575 F.3d 834, 844 (8th Cir. 2009) (affirming finding of probable cause where affidavit in support of search warrant application referred to IP address that had been used to access child pornography sites was traced to a defendant); see also e.g., United States v. Freeman, No. 10-cr-68 (JRT/RLE), 2010 WL 4386897, at *11 (D.Minn. May 13, 2010) (finding nexus between child pornography and a computer at a physical address based on an email account, an IP address, and the home address to which the IP address was assigned), adopted by 2010 WL 4386874 (D.Minn. Oct. 28, 2010). Investigator Pauly's reference in the affidavit to IP address 71.83.33.81 as having been assigned to Defendant's home address during the time period in which Officer Hansen downloaded copies of payload files from a host computer at that IP address is sufficient to create a nexus between those payload files and Defendant's residence. Similarly, Investigator Pauly's reference in the affidavit to IP address 24.158.30.34 as having been assigned to Computer Renaissance at 2208 Mountain Shadow Drive in Duluth, Minnesota, during the period in which Officer Hansen

downloaded copies of the payload files from a host computer at that IP address is sufficient to create a nexus between the payload files and the address of Defendant's employer.

Defendant next argues, in essence, that there were neither enough files to create probable cause here, nor were the payload files sufficiently explicit as to be considered pornography. "[T]he Eighth Circuit has held that a single image of child pornography can suffice to provide probable cause to search a suspect's computer." United States v. Needham, No. CRIM. 13-111 (JRT/LIB), 2013 WL 4519414, at *9 (D. Minn. Aug. 26, 2013) (citing United States v. McArthur, 573 F.3d 608, 613–14 (8th Cir. 2009) (upholding as lawful under the totality of the circumstances a search of a defendant's home computer where defendant was found in public with a single computer-edited image of child pornography in his wallet, the defendant had been convicted of prior sex offenses, and the affidavit indicated that people who tend to view child pornography tend to hoard secreted images in their homes)). Accordingly, the mere fact that few images or even a single image of child pornography was discovered on the computers will not prevent a finding that Judge Larson had a sufficient basis to conclude that probable cause existed.

Defendant also contends that the images in this case should not be considered child pornography. For the purpose of federal child pornography charges "child pornography" means any visual depiction . . . where . . . the visual depiction involves the use of a minor engaging in sexually explicit conduct. 18 U.S.C. § 2256(8)(A-C). In the context of digital images, "sexually explicit conduct" includes "graphic or simulated lascivious exhibition of the genitals or pubic area of any person[.]"18 U.S.C. § 2256(2)(B)(iii).

The Eighth Circuit has explained:

> Nudity alone does not fit this description; there must be an "exhibition" of the genital area and this exhibition must be "lascivious." A picture is "lascivious"

> only if it is sexual in nature. In attempting to determine the limits of this category of sexually explicit conduct, we find helpful the six criteria suggested in United States v. Dost, 636 F.Supp. 828, 832 (S.D.Cal.1986), aff'd sub nom. United States v. Wiegand, 812 F.2d 1239 (9th Cir.1987), cert. denied, 484 U.S. 856, 108 S.Ct. 164, 98 L.Ed.2d 118 (1987). We have found that when the child is nude or partially clothed, when the focus of the depiction is the child's genitals or pubic area, and when the image is intended to elicit a sexual response in the viewer, the depiction is lascivious. The other criteria outlined in Dost include a sexually suggestive setting, inappropriate attire or an unnatural pose for a child, and a suggestion of sexual coyness or willingness to engage in sexual behavior. [A]ll six [Dost] factors need not be present in order to bring the depiction under the proscription of the statute. Furthermore, the Dost factors are not exhaustive, as other factors may be relevant, depending upon the particular circumstances involved. Thus, the "inquiry will always be case-specific.

United States v. Wallenfang, 568 F.3d 649, 657-58 (8th Cir. 2009) (citations and quotation marks omitted).

In the present case, one of the payload files downloaded from the host computer at IP address 24.158.30.34, Defendant's employer, depicted a partially clothed to nude female between the ages of twelve and fourteen posing for the camera, with a focus on her exposed genitalia and anus. Thus, two of the Dost factors were clearly present in that picture. Investigator Pauly's affidavit does not say that the child was in a pose intended to elicit a sexual response, but does state the child was posing for the camera. Given the presence of two of the Dost factors, the ambiguous nature of the way in which the child's pose was described, and the absence of any other description regarding factors that would detract from the clear presence of two of the two present factors, the Court concludes that Judge Larson had a substantial basis to conclude that the image depicted a minor engaging in lascivious exposition of the her genitals, such as to constitute child pornography. See United States v. Kemmerling, 285 F.3d 644, 646 (8th Cir. 2002) ("A factfinder could decide . . . that the other pictures are lascivious because they are of children who are nude or partially clothed, the focus of the images is the child's genitals or pubic area, and their purpose appears to be to elicit a sexual response from the viewer. These

images were not designed, for instance, simply to provide a clinical view of the portions of the children's anatomy that are pictured.").

The fact that the file was hosted on the computer at IP address 24.158.30.34 is a substantial basis for Judge Larson to conclude to conclude that evidence of a crime could be found on that computer.

In addition, the presence of that image on the computer at the 24.158.30.34 IP address, which happens to be Defendant's employer, together with Defendant's previous convictions for criminal sexual conduct involving a minor, his lifetime status as a predatory offender, his violation of a condition of his probation by having internet access at home, the presence of images displaying prepubescent females in lingerie and in partially undressed, sexually suggestive manners on the computer at his home computer 71.83.33.81 IP address, the fact that the home computer at the 71.83.33.81 IP address was also running a P2P file sharing program on the same file sharing network as the computer at Defendant's workplace the 24.158.30.34 IP address, and Investigator Pauly's statements in the search warrant application that based on her experience and training computer transfer and digital copying via the internet is the preferred method of distributing pornography, is a sufficient basis, under the totality of the circumstances, for Judge Larson to conclude that there was a reasonable probability that evidence of a crime could be found on the computer at Defendant's residence as well. See McArthur, 573 F.3d at 613-14 (upholding probable cause to search a home computer where defendant found in personal possession of a single hard copy image of computer-modified child pornography, the defendant had multiple previous convictions, and affiant stated that images of child pornography are likely to be hoarded by persons interested in those materials and secreted in secure places like a private residence); see also United States v. Chrobak, 289 F.3d 1043, 1046 (8th Cir. 2002) (finding a

sufficient nexus between the transmission of pornographic files via a defendant's email address and the defendant's home computer in affiant's statement that the email address belonged to the defendant, evidence that the defendant lived at his home address, and a statement that, in her experience, pedophiles maintain their child pornography in a secure place).

Based on the foregoing, Judge Larson had a substantial basis to conclude there was a reasonable probability that evidence of a crime could be found on computers at both Defendant's employment and Defendant's residence.

However, even if the Court were to find that probable cause did not exist to believe that evidence of contraband could be found on the computers at Defendant's workplace and Defendant's residence, the Court concludes that the Defendant's motion to suppress evidence gathered as a result of the search warrants should still be denied under the Leon good faith exception.

"Under the Leon good-faith exception, disputed evidence will be admitted if it was objectively reasonable for the officer executing a search warrant to have relied in good faith on the judge's determination that there was probable cause to issue the warrant." Grant, 490 F.3d at 632 (citing United States v. Leon, 468 U.S. 897, 922 (1984)). Even if the Court were now to conclude here that the affidavit supporting the May 22, 2014, search warrants did not set forth facts within their four corners sufficient to demonstrate probable cause to search the computers at Defendant's residence and workplace, on the present record, law enforcement's good-faith reliance on the warrants issued by Judge Larson to search those computers militates against suppressing any evidence obtained in the search. See Leon, 468 U.S. at 919-921 (exclusionary rule does not apply "when an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope"). See also United States v.

Johnson, 219 F.3d 790, 791 (8th Cir. 2000) ("Even if we thought the warrant affidavit did not establish probable cause, the good faith exception to the warrant requirement would apply because the affidavit was sufficient to allow an officer to reasonably believe probable cause existed."); United States v. Rugh, 968 F.2d 750, 753 (8th Cir. 1992) ("When police objectively and reasonably believe that probable cause exists to conduct a search based on an issuing judge's determination of probable cause, evidence seized pursuant to the ultimately invalid search warrant need not be suppressed.").

Investigator Pauly's affidavits in support of the applications for the search warrants indicates that she presented Judge Larson with specific facts indicating that at least one computer associated with Defendant contained an image bearing recognized hallmarks of child pornography, in that it clearly embodied two of the Dost factors and was ambiguous as to a third factor. The affidavits also indicated that, despite being prohibited from doing so as a result of a previous conviction of criminal sexual conduct involving a minor, Defendant had internet access at his home and that a computer at Defendant's residence was on the same file sharing network as the computer at Defendant's workplace, running a P2P file sharing software and hosting images of prepubescent females dressed in bathing suits and a video file in which a prepubescent girl is dancing with the top of her dress down to reveal her bare chest to the camera. Accordingly, when executing the search warrants for Defendant's residence and workplace, law enforcement relied in good faith on the search warrant issued by Judge Larson.

D. Conclusion

Because the affidavits authored by Investigator Pauly provided probable cause to believe that evidence of a crime could be found on a computer at Defendant's residence and at Defendant's workplace, and law enforcement, in any event, relied in good faith on Judge

Larson's issuance of the May 22, 2014 search warrants, the Court recommends **DENYING** Defendant's Motion to Suppress Any Evidence Obtained as a Result of Any Illegal Searches, [Docket No. 16].

III. DEFENDANT'S MOTION TO SUPPRESS STATEMENTS, [DOCKET NO. 17].

Defendant next moves the Court for an order suppressing any statement he made in violation of his rights under the Fourth, Fifth, or Sixth Amendments. (See Defendant's Motion to Suppress Statements, [Docket No. 17]). Specifically, Defendant argues solely that his statements must be suppressed as the product of the execution of the unlawful May 22, 2014, search warrants of the computers at his home and workplace.

A. Standard of Review

Evidence that law enforcement obtains in violation of the Fourth Amendment is subject to the exclusionary rule and, as such, "cannot be used in a criminal proceeding against the victim of the illegal search and seizure." United States v. Calandra, 414 U.S. 338, 347 (1974). "[T]he exclusionary rule reaches not only primary evidence obtained as a direct result of an illegal search or seizure, but also evidence later discovered and found to be derivative of an illegality or 'fruit of the poisonous tree.'" Segura v. United States, 468 U.S. 796, 804, 104 S.Ct. 3380, 82 L.Ed.2d 599 (1984) (citations omitted). In addition, "[v]erbal statements obtained as a result of a Fourth Amendment violation are as much subject to the exclusionary rule as are items of physical evidence discovered during an illegal search." United States v. Riesselman, 646 F.3d 1072, 1078-79 (8th Cir. 2011) (quoting United States v. Yousif, 308 F.3d 820, 832 (8th Cir. 2002)).

B. Analysis

Defendant's sole argument in support of his motion to suppress his statements is that the statements are the product of the execution of the May 22, 2014 search warrants, which were unlawful as not being supported by probable cause. The Court has, however, concluded that those warrants were supported by probable cause and their execution was, therefore, lawful. As such, Defendant's statements were not the product of unlawful searches.

Because the statements that Defendant seeks to suppress were not the product of unlawful conduct in violation of Defendant's rights, the Court recommends **DENYING** Defendant's Motion to Suppress Statements, [Docket No. 17].

IV. CONCLUSION

Based on the foregoing and all the files, records, and proceedings herein, **IT IS HEREBY RECOMMENDED** that:

1. Defendant's Motion to Suppress Any Evidence Obtained as a Result of Any Illegal Searches, [Docket No. 16], be **DENIED**; and,
2. Defendant's Motion to Suppress Statements, [Docket No. 17], be **DENIED**.

Dated: November 4, 2014

s/Leo I. Brisbois
Leo I. Brisbois
U.S. MAGISTRATE JUDGE

N O T I C E

Pursuant to Local Rule 72.2(b), and as discussed with counsel at the time of the October 27, 2014, motions hearing, in light of the pending December 1, 2014, trial date, a shortened period for objections to this Report and Recommendation is necessitated. Therefore, any party may object to this Report and Recommendation by filing with the Clerk of Court, and serving all parties **by November 7, 2014** a writing that specifically identifies the portions of the Report to which objections are made and the bases for each objection. A party may respond to the objections **by November 10, 2014**. Written submissions by any party shall comply with the

applicable word limitations provided for in the Local Rules. Failure to comply with this procedure may operate as a forfeiture of the objecting party's right to seek review in the Court of Appeals. This Report and Recommendation does not constitute an order or judgment from the District Court, and it is therefore not directly appealable to the Court of Appeals.